**Парламентское собрание Союза Беларуси и России**

**Постоянный Комитет Союзного государства**

**Оперативно-аналитический центр**
**при Президенте Республики Беларусь**

**Государственное предприятие «НИИ ТЗИ»**

**Полоцкий государственный университет**


# КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

**УДК 004(470+476)(061.3)**
**ББК 32.81(4Беи+2)**

**ISBN 978-985-531-564-4**

# РЕСПУБЛИКАНСКИЙ УДОСТОВЕРЯЮЩИЙ ЦЕНТР ГОСУДАРСТВЕННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОТКРЫТЫМИ КЛЮЧАМИ ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ РЕСПУБЛИКИ БЕЛАРУСЬ – ПОСТАВЩИК СЕРВИСОВ ДОВЕРИЯ

А.В. ШИБКОВ

*Оперативно-аналитический центр при Президенте Республики Беларусь*

Глобальные тенденции цифровой трансформации общества определяют, что взаимодействие между субъектами информационных отношений все более смещается к их удаленному взаимодействию посредством различных информационных систем. Такое взаимодействие требует применения определенных решений и механизмов, позволяющих установить определенную степень доверия между этими субъектами. В качестве субъектов взаимодействия могут быть как люди, так и определенные информационные ресурсы и сервисы. Для установления доверительных отношений субъекты должны быть однозначно идентифицированы в информационных системах, посредством которых они общаются.

Некоторые способы идентификации в информационных системах основаны на использовании ассиметричной криптографии (так называемой криптографии с открытыми ключами), а точнее на использовании сертификатов открытых ключей (СОК).

Для использования таких технологий, как правило, создается инфраструктура открытых ключей. Причем, если таких инфраструктур несколько, необходимо еще устанавливать доверие между ними.

В Республике Беларусь создана и с 30 июня 2014 г. функционирует национальная инфраструктура открытых ключей – Государственная система управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь (ГосСУОК).

Порядок ее функционирования определяется следующими нормативными правовыми актами:

Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

Указ Президента Республики Беларусь от 8 ноября 2011 г. № 515 «О некоторых вопросах развития информационного общества в Республики Беларусь» (определено, что Республиканское унитарное предприятие «Центр электронных услуг» осуществляет функции оператора корневого и иных удостоверяющих центров ГосСУОК, национального оператора по признанию подлинности электронных документов при межгосударственном электронном взаимодействии);

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118 «Об утверждении Положения о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 ноября 2013 г. «Об утверждении инструкции о порядке проведения аккредитации поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и осуществления контроля за соблюдением условий аккредитации»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 26 июня 2014 г. № 54 «О некоторых вопросах функционирования корневого

удостоверяющего центра Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь» (утверждены Политика применения сертификатов открытых ключей, изданных корневым УЦ ГосСУОК и Регламент корневого УЦ ГосСУОК).

Кроме того, требования установлены в технических нормативных правовых актах.

В настоящее время ГосСУОК представляет из себя иерархическую инфраструктуру открытых ключей и состоит из корневого и республиканского удостоверяющих центров (УЦ), а также разветвленной сети регистрационных центров (РЦ).

Информация о ГосСУОК содержится на следующих информационных ресурсах: http://oac.gov.by/tzi/gossuok; https://nces.by/pki.

Основными функциями корневого УЦ являются издание, распространение, предоставление информации о статусе, отзыв и хранение СОК республиканского УЦ, кросс-сертификация (установление отношений доверия) с внешними инфраструктурами открытых ключей, в том числе с иностранными.

Основными функциями республиканского УЦ являются управление СОК РЦ, центра атрибутных сертификатов, физических и юридических лиц, сервисов (приложения, серверы или устройства), функции РЦ.

Основной функцией РЦ является проверка информации, вносимой в СОК, формирование и регистрация заявок на издание и отзыв СОК (достоверное подтверждение принадлежности открытого ключа его владельцу).

По состоянию на 12 апреля 2017 г. в ГосСУОК аккредитовано девять юридических лиц, предоставляющих услуги РЦ, в составе 33 удаленных рабочих мест регистраторов:

республиканское унитарное предприятие «Национальных центр электронных услуг» – 1.

республиканское унитарное предприятие «Информационно-вычислительный центр Министерства финансов Республики Беларусь» – 5;

республиканское унитарное предприятие электросвязи «Белтелеком» – 5;

научно-производственное республиканское унитарное предприятие «Научно-исследовательский институт технической защиты информации» – 1;

республиканское унитарное предприятие «Информационно-издательский центр по налогам и сборам» – 17;

Государственный пограничный комитет Республики Беларусь – 1;

республиканское унитарное предприятие «Производственное объединение «Белоруснефть» - 1 (г.Гомель);

унитарное предприятие по оказанию услуг «Велком» - 1 (г.Минск);

совместное общество с ограниченной ответственностью «Мобильные ТелеСистемы» - 1.

С 30 декабря 2016 г. республиканским УЦ издаются сертификаты открытых ключей юридических лиц, физических лиц (в том числе для использования Sim-ID), атрибутные сертификаты, сертификаты сервисов (так называемые технологические сертификаты). Профили этих сертификатов определены в приложениях к соответствующим политикам применения сертификатов открытых ключей, атрибутных сертификатов, издаваемых республиканским УЦ. Кроме этого республиканским УЦ реализованы сервисы OCSP.

СОК по своей сути это электронный документ, который удостоверен электронной цифровой подписью (ЭЦП) республиканского УЦ, и связывает имя субъекта с его личным ключом. В СОК содержится ряд параметров, позволяющих обеспечить доверие

к СОК субъекта (имя субъекта, имя эмитента, уникальный открытый ключ субъекта и другие), посредством формирования цепочки сертификатов и единую точку доверия в ГосСУОК – корневой УЦ.

Таким образом, используя СОК можно идентифицировать и аутентифицировать в информационной системе субъекта-владельца этого сертификата, а также проверить действительность ЭЦП поступившего электронного документа.

Но сертификат открытого ключа не всегда определяет полномочия его владельца совершение тех либо иных действий в информационной системе, а также в каком статусе этот владелец выступает.

Ответы на эти вопросы может дать атрибутный сертификат. Атрибутный сертификат обязательно должен быть связан с СОК субъекта и по своей сути также является электронным документом, который удостоверен ЭЦП центра атрибутных сертификатов, и содержит структуру данных, связывающих определенные значения атрибутов с идентификационной информацией о держателе. В качестве атрибутов могут быть назначены определенные привилегии (полномочия или свойства), которые могут быть делегированы, а также определенные роли. Архитектура атрибутных сертификатов описана в государственном стандарте СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов». Различают следующие модели инфраструктуры управления привилегиями: общая модель, модель системы управления доступом, модель делегирования привилегий, модель назначения привилегий группе субъектов, модель ролей, модель взаимодействия доменов. Атрибутные сертификаты выпускает республиканский УЦ.

В отдельных случаях возникает ситуация, когда субъектом А подписан электронный документ (ЭД) и отправлен субъекту Б. За время доставки ЭД от субъекта А субъекту Б может истечь срок действия СОК субъекта А либо СОК может быть отозван. Если субъект Б осуществляет проверку действительности ЭЦП с использованием списков отозванных сертификатов и СОК субъекта А своевременно помещен в этот список, тогда при проверке подлинности ЭД полученного от субъекта А, ЭЦП субъекта А будет считаться недействительной. Но на момент подписания СОК субъекта А был действительным. Для обеспечения такого уровня доверия существует сервис OCSP, основанный на использовании онлайнового протокола проверки статуса сертификата, описанного в государственном стандарте СТБ 34.101.26-2012. Фактически с использованием сервиса OCSP можно проверить действительность СОК в момент подписи. Для этого выстраивается клиент-серверная архитектура, состоящая из OCSP-сервера и OCSP-клиентов. Инициатором OCSP-запроса выступает OCSP-клиент. На полученный OCSP-запрос OCSP-сервер формирует и отправляет инициатору OCSP-ответ, так называемую квитанцию OCSP, содержащий такие компоненты как CertID, ResponderData.

При информационных взаимоотношениях возникают ситуации, когда необходимо подтвердить существование информационного объекта, например, электронного документа с хэш-значением в определенный момент времени. Для таких целей формируется штамп времени. Служба TSP стандартизирована в RFC3161. В Республике Беларусь проводится стандартизация этого протокола, разработан проект СТБ 34.101.ts.

Как уже упоминалось, между инфраструктурами открытых ключей, особенно при межгосударственном информационном взаимодействии, также необходимо обеспечивать доверия, в частности для обеспечения признания подлинности электронных документов, изданных в иностранных государствах. Данная задача может быть реализована с использованием службы DVCS, реализующей Data Validation and Certification Server Protocol, описанный в RFC3029.